Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 19 July 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- Reuters reports that Los Alamos National Laboratory in New Mexico, a key U.S. center for nuclear weapons research, has temporarily ceased all classified work after vital data was reported missing recently from a research area. (See item 3)
- The Record Journal reports that the postal distribution plant on Research Parkway will be the first in Connecticut to receive a new system designed to detect anthrax and other dangerous contaminants sent through the mail. (See item 13)
- SearchDomino.com reports that a trio of newly discovered vulnerabilities in the IBM Lotus Notes R6.x client could put sensitive information on users' PCs at risk. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 17, San Francisco Chronicle* — **Officials hope nuclear rods are in pool. Pacific Gas & Electric officials are seeking three missing radioactive portions of a used nuclear fuel rod from the long−defunct Humboldt Bay nuclear power reactor near Eureka, CA. Each fragment −− 18 inches long and about a half−inch thick −− contains used uranium fuel inside a stainless−steel cladding,** utility officials said in a statement Friday, July 16. For now, utility officials' working hypothesis is that the rod fragments will eventually be found somewhere inside the cluttered reactor pool at the plant. Still, they can't totally rule out an

unsettling possibility −− that at some time over the last third of a century, the rods somehow left the plant for points uncertain. Analysts for the utility analysts noticed "the first indication of a discrepancy" in their records on June 23. Since Wednesday, July 7, they have used robotic arms to search for the rod fragments inside the reactor pool. The 65−megawatt Humboldt Bay reactor generated energy for consumers along the Northern California coast and points inland from 1963 to 1976. Afterward the reactor was shut down, but the used nuclear fuel is still stored in the pool.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2004/07/17/BAGP 27NBQ91.DTL

2. *July 17, Xinhuanet* — **Russia to increase oil export duty. Russia will increase oil export duty by 68 percent to a record high of $69.90 per ton beginning on August 1,** the Russian government announced Saturday, July 17. The new oil export duty, up from the current $41.60, was calculated based on Russian oil prices for May−June, the Interfax news agency quoted Prime Minister Mikhail Fradkov's press service as reporting. Russia revises its oil export duty every two months in compliance with its oil prices in the global market. **Russia is the world's second largest oil exporter after Saudi Arabia.** Deputy Prime Minister Alexander Zhukov pledged in May that Russia will strive to export more oil due to a good market prospect, but the size of the increase required further analysis.
Source: http://news.xinhuanet.com/english/2004−07/17/content_1610060 .htm

3. *July 15, Reuters* — **U.S. nuclear lab temporarily halts secret work. The Los Alamos National Laboratory in New Mexico, a key U.S. center for nuclear weapons research, has temporarily ceased all classified work after vital data was reported missing recently from a research area,** lab officials said on Thursday, July 15. The lab said it learned of two missing data storage disks on Thursday, July 7, during an inventory check. "Until such time as we are confident that we are addressing this issue, then all activities with respect to classified materials have been put on hold," said Gerald Parsky, chairman of the Regents of the University of California,which manages Los Alamos. Los Alamos spokesperson Kevin Roark said "fewer than 20" staffers have had their lab access suspended pending the results of the inquiry. "Where in the past, most of the issues were associated with inventory errors and that sort of thing, I have a clear indication here that people did not follow the rules as to the chain of custody and keeping track and doing the proper documented transfer of material," Lab director Gerald Nanos said. **Officials said, however, that they had no indication that the sensitive data had been taken outside of the facility.**
Source: http://www.reuters.com/newsArticle.jhtml;jsessionid=FKJR1VTK 04T34CRBAELCFEY?type=topNews&storyID=5685536&pageNumber=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *July 16, Associated Press* — **Probe into fatal mill accident brings new safety warning. A two year federal probe into a fatal paper mill accident in Pennington, AL, has led to a new federal government safety bulletin on handling deadly sodium hydrosulfide**. The U.S. Chemical Safety and Hazard Investigation Board on Friday, July 16, released its bulletin that warns of the dangers of the chemical and sets out safe practices to prevent accidents when handling it. The board's action follows a January 16, 2002 hydrogen sulfide leak that caused

two deaths and eight injuries at a Georgia−Pacific Corp. plant. Federal investigators found 45 accidents linked to sodium hydrosulfide that have caused 32 deaths and 176 injuries since 1971. Pulp mills typically use hydrogen sulfide and other chemicals to turn wood into raw fiber for paper.
Source: http://www.miami.com/mld/miamiherald/business/9172896.htm?1c

[Return to top]

Defense Industrial Base Sector

5. *July 16, American Forces Press Service* — **IRR call−up allows U.S. Army to build cohesive teams.** The U.S. Army's call−up of several thousand Individual Ready Reserve (IRR) soldiers will allow that service to keep cohesive teams in the National Guard and Army Reserve together, the service's number two general said Thursday, July 15. Army Vice Chief of Staff General Richard A. Cody said that **the activation will allow the IRR to "fill critical billets and spaces in the units we call up for our rotation for Operation Iraqi Freedom 3 and Operation Enduring Freedom 6."** Cody said letters went out July 6 to 5,674 members of the IRR, soldiers who have completed an active−duty enlistment but still are within eight years of when they entered the military. Of those who received the letters, Cody said, roughly 4,000 will be brought to active duty. Most of those will be in the specialties of military intelligence, engineers, truck drivers, and other "combat service support" forces, he said. He explained that **having access to IRR soldiers allows the military to fill holes in units without having to call up other units simply to make up for shortfalls "so we have less disruption across the force," he said.**
Source: http://www.defenselink.mil/news/Jul2004/n07162004_2004071602 .html

[Return to top]

Banking and Finance Sector

6. *July 16, Finextra Research* — **ATM skimmers go hi−tech down under.** Australian police have described an ATM skimming device uncovered in Sydney, which is estimated to have recorded the details of up to 1000 customers, as one of the most advanced to date. The system uses a pin−hole camera to record the personal identification numbers (PINs) and a magnetic strip reader to copy details on the cards. The thieves can then burn the data onto a magnetic strip card to access bank accounts. Michael Boutouridis, from the NSW fraud squad, said **the new skimming device was one of the first to have its own memory system and showed that technology used by fraudsters has advanced.** "With the other machines we have found, they would have to remain close by to watch the details...But this one can be used over a long period of time, with the information stored on tape and on chips inside," he says.
Source: http://www.finextra.com/fullstory.asp?id=12184

7. *July 16, Financial Times* — **PNC to buy Riggs bank. Riggs National on Friday, July 16, agreed to be sold for $779 million in stock and cash to PNC Financial of Pennsylvania. The deal will end the Washington, D.C., lender's 165−year history as an independent company,** which was recently tainted by revelations that it failed to respect anti−money

laundering laws. Recently, a congressional report slammed Riggs for not informing regulators that it was handling tens of millions of dollars for Augusto Pinochet, the former Chilean dictator. In May, Riggs was ordered to pay a record fine of $25m for money−laundering violations related to diplomats' accounts. PNC expects the bank's international and embassy units to be divested before the deal closes. **In a sign of PNC's intention to break with the past, the Riggs name will be replaced by that of the Pittsburgh−based bank.** By buying Riggs, PNC, which is the 15th largest U.S. bank with $74bn in assets, will add 50 branches to its strong presence in the mid−Atlantic region of the U.S. PNC said the deal is expected to close early next year.
Source: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1087373775474&p=1012571727088

8. *July 16, vnunet.com (UK)* — **Worried firms consider e−mail boycott. Six out of ten companies in the United Kingdom claim they will give up e−mail if the threat posed by viruses, spam and other unwanted content is not contained and a viable alternative emerges**. Responding to an e−mail security survey carried out by MessageLabs, a further 40 percent said they feel worried by the current e−mail security threat to their business, with only 29 percent feeling optimistic. Over 20 percent of firms responding to the research indicated that online fraud, such as phishing and identity theft, will be the greatest threat. The leakage of confidential or sensitive information was rated by 18 percent as the main issue, with 15 percent stating that it would be the potential for industrial espionage. The survey reveals continued concern over levels of spam, with over 40 percent of respondents predicting that levels of junk e−mail will more than double over the next ten years.
Source: http://www.vnunet.com/news/1156684

[Return to top]

Transportation Sector

9. *July 16, Transportation Security Administration* — **TSA awards grant for research and development of port security technology.** The Transportation Securtiy Administration (TSA) announced Friday, July 16, that it has awarded the Regional Maritime Security Coalition (RMSC), of Portland, OR, $1.62 million for research and development of port security enhancements in the Northwest. The grant is to go toward the development of a prototype multi−jurisdictional, multi−agency Cargo Information Action Center (CIAC) for the 22 ports in the Columbia−Snake River System that stretches from the Pacific Ocean at Astoria, OR, to Lewiston, ID. **This grant will improve communications and coordination throughout the tri−state (WA, OR and ID) region, employing a secure wide−area system**.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 00b8cc9

10. *July 15, Department of Transportation* — **DOT announces grants to improve runways, taxiways, enhance safety at three New Jersey airports.** The Department of Transportation (DOT) announced Thursday, July 15, grants totaling $4.8 million for runway and taxiway upgrades to expand capacity and enhance safety at three New Jersey airports: Millville Municipal, Cape May County, and Hammonton Municipal. **The grants will provide funding for projects such as rehabilitating runway and taxiway lighting, improving taxiways and drainage systems, and land acquisition**. The funds come from the Airport Improvement

Program of the DOT's Federal Aviation Administration (FAA).
Source: http://www.dot.gov/affairs/dot10004.htm

11. *July 15, Department of Transportation* — **DOT takes enforcement action against two pipeline companies for safety violations.** The Department of Transportation (DOT) announced Thursday, July 15, enforcement actions against two pipeline operators, Kinder Morgan Energy Partners, LLC, and Puget Sound Energy, Inc. The DOT's Research and Special Programs Administration (RSPA) cited the two companies for a range of pipeline safety violations. The enforcement actions, announced in Tuscon, AZ, include a Notice of Probable Violation issued to Kinder Morgan following inspections of the company's entire hazardous liquid pipeline system. **Of the most significant violations found were inadequate consideration of significant pipeline integrity threats, including seam defects, stress corrosion cracking and deficient risk assessment. A metallurgical analysis of failed pipe material concluded stress corrosion cracking was the cause of a July 30, 2003, Kinder Morgan pipeline break in Tucson**. RSPA also issued a Final Order against Puget Sound for violations of federal drug and alcohol requirements, failure to participate in a qualified one−call program, and failure to establish a continuing pipeline education program, among other violations.
Source: http://www.dot.gov/affairs/rspa0304.htm

12. *July 15, Department of Transportation* — **DOT announces grants to expand capacity, enhance safety at New Mexico airports.** Federal grants totaling $10.1 million will help to expand capacity and enhance safety at airports throughout New Mexico, Department of Transportation (DOT) Secretary Norman Y. Mineta announced Thursday, July 15. **Twenty−two airports will receive money for several projects, including rehabilitation and extension of runways, taxiways and aprons, installation of guidance systems, and acquisition of equipment and land**. The funds come from the Airport Improvement Program of the DOT's Federal Aviation Administration (FAA). In addition to individual airport grants, the state of New Mexico received $110,200 to prepare airport master plan studies for airports in Hatch, Las Vegas, Los Alamos and Springer.
Source: http://www.dot.gov/affairs/dot9904.htm

[Return to top]

Postal and Shipping Sector

13. *July 18, Record Journal (CT)* — **Testing gear set for USPS terminal. The postal distribution plant on Research Parkway will be the first in Connecticut to receive a new system designed to detect anthrax and other dangerous contaminants sent through the mail.** The Biohazard Detection System, which has been piloted in New York and other parts of the country, is scheduled to be installed in the Southern Connecticut Processing and Distribution Center the first week of August. The detection system is a series of machines retrofitted to existing equipment that sorts incoming mail, said U.S. Postal Service (USPS) spokesman Carl Walton. The machine tests for biological hazards by taking air samples every 45 seconds, he said. A ventilation and filtration system will also be installed to complement the system, officials said.
Source: http://www.record−journal.com/articles/2004/07/17/news/news0 4.txt

[Return to top]

Agriculture Sector

14. *July 16, Caspar Star Tribune (WY)* — **Agency fine tunes search for wasting disease.** The Wyoming Game and Fish Department plans to reduce by several thousand the number of deer and elk that will be tested statewide this fall for the fatal brain ailment Chronic Wasting Disease (CWD). **The agency's surveillance strategy is shifting away from general mass sampling and will now focus more on tracking the disease's movement west across the Continental Divide and north up from Colorado, agency officials said.** Last fall, the department took samples from just over 6,000 hunter−killed deer and elk in a first−ever, massive surveillance effort aimed at tracking the disease in Wyoming. The surveillance revealed CWD in several new areas of the state. CWD has been endemic to a 12,000−square−mile area of southeastern Wyoming and northeastern Colorado for more than 30 years. But the movement of the disease to such places as the Black Hills of South Dakota and to the west slope of the Continental Divide has wildlife managers concerned about its spread.
Source: http://www.casperstartribune.net/articles/2004/07/16/news/wyoming/6c8f4928f7a7134587256ed300064aa3.txt

15. *July 15, University of Idaho* — **Scientists join forces to fight invasive species. Invasive species such as white pine blister rust, spotted knapweed and whirling disease in trout, as well as declining populations of plants and animals, are the focus of a new research center at the University of Idaho (UI).** Degradation or destruction of Idaho's natural resource base is one of the greatest biological problems facing the state, UI researchers say. They predict the incidence of introduced −− and consequently, destructive −− species will only increase in years to come, given the increased mobility of human populations and globalized commercial traffic. Statistics gathered by the Idaho Invasive Species Council support that claim. **The group examined one 1999 survey that estimated the annual economic impact nationwide of alien species at some $138 billion in direct losses to agriculture and industry.** Losses due to noxious weeds alone are estimated to cost the state approximately $3 million annually. Another focus of the center will be to provide critical genetic analysis for the management of small plant and animal populations. Declining elk herds, fish stocks, white bark pine populations, and other threatened and endangered species pose major challenges to natural resource managers in Idaho.
Source: http://www.enn.com/direct/display−release.asp?objid=D1D1366D000000FDC4A35BE677B9D819

[Return to top]

Food Sector

16. *July 16, Oster Dow Jones Commodity News* — **Auditors criticize approach to meat recall records. Because of poor record−keeping and a "careless approach" by U.S. Department of Agriculture (USDA) officials, the government can't be sure how much meat is removed from the market in recalls, the agency's top internal watchdog said.** A report by the

USDA's inspector general's office on a 2002 recall of 27.4 million pounds of sliced deli poultry from a Wampler Foods plant in Franconia, Pa., found discrepancies or missing data in 389 of 582 department records tracking the results. "We attributed this high error rate to the careless approach compliance officers and supervisory personnel took in overseeing the recall," the report said. "Until it corrects the problems we identified, Food Safety and Inspection Service's (FSIS) conclusions regarding the effectiveness of food safety recalls may be based on inaccurate and incomplete information." The FSIS signed off in July 2003 on terminating the recall after Wampler said it had recovered more than 5.5 million pounds of the product. Because of the paperwork errors "FSIS did not have reasonable assurance that potentially adulterated product bearing the USDA seal of inspection had been retrieved," the inspector general's report said.
Source: http://www.agprofessional.com/show_story.php?id=26230

17. *July 16, Food and Drug Administration* — **FDA issues alert on foodborne illness outbreaks in Pennsylvania and mid−Atlantic states. The U.S. Food and Drug Administration (FDA) is issuing an alert to consumers that 57 cases of salmonellosis may be associated with food purchased at deli counters contained in Sheetz Gas Station locations in Pennsylvania, Maryland, and West Virginia between July 2 and July 9.** The agency is working with the Pennsylvania Department of Health, other state and county agencies, and the U.S. Centers for Disease Control and Prevention to determine the cause and scope of the problem. At this time no product has been implicated and the investigation is continuing. Salmonella is an organism which causes serious and sometimes fatal infection in young children, frail or elderly people, and others with weakened immune systems. In rare circumstances, infection with Salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis.
Source: http://www.fda.gov/bbs/topics/news/2004/NEW01090.html

18. *July 16, Cornell University* — **Once discovered, listeria can continue to contaminate food. Despite the efforts of food retailers and food−processing plant managers to maintain a clean environment, strains of the pathogen Listeria monocytogenes can persist for up to a year or longer, according to Cornell University food scientists.** "This is disturbing because this points the finger at retail stores and some processors as a continuing source of food contamination," says Brian D. Sauders, a Cornell doctoral candidate in food science who worked on the study with Martin Wiedmann, D.V.M., Cornell assistant professor of food science. Sauders and Wiedmann examined specific strains of L. monocytogenes that had been found in 125 foods in 50 retail food stores and seven food−processing plants in New York state examined by inspectors of the New York State Department of Agriculture and Markets. The inspectors found the bacteria during routine surveys, sanitary inspections and as a result of consumer complaints between 1997 and 2002. The bacterium was found directly on food in 47 of 50 retail food stores, including 20 food stores where the bacterium was found on several foods. When the 50 stores were re−inspected weeks, months or even a year later, about 34 percent had persistence of the same strains of Listeria. Of the seven food−processing plants where Listeria was found, three had persistent strains of the bacterium.
Source: http://www.sciencedaily.com/releases/2004/07/040716081935.ht m

19. *July 15, Food Safety and Inspection Service* — **FSIS detains adulterated pork products. The Food Safety and Inspection Service (FSIS) Thursday, July 15, began to detain an**

undetermined amount of fried pork fat that was produced in a federal establishment without the presence of U.S. Department of Agriculture inspectors. These products are considered to be adulterated and FSIS encourages consumers to avoid eating them and discard them. The establishment in question goes by the name of DownHome HomeBoys in St. Louis, MO. FSIS has also withheld the marks of inspection and suspended the assignment of inspectors from the establishment. Without federal inspection, products cannot legally be distributed into commerce. **On July 13, FSIS program employees were refused entry to examine the facilities, inventory, and records at this establishment. This is a violation of the Federal Meat Inspection Act.** When an establishment applies for a grant of inspection, it is understood that every applicant will be held responsible for adhering to this law and other applicable regulations if inspection is granted. Consumers should look for products labeled, "Downhome, Hot, Krispy, Snacklin' Cracklin' Fried Out Pork Fat with attached skin." FSIS' detention of these products is underway in multiple states.
Source: http://www.fsis.usda.gov/News_&_Events/NR_071504_01/index.as p

[Return to top]

Water Sector

20. *July 16, Water Tech Online* — **Water company expands with $63 million purchase. Southwest Water Company has completed its acquisition of a Texas utility consisting of 86 water systems and 11 wastewater systems from Tecon Water Holdings, LP, according to a news release.** The approximately $63 million purchase price was paid by the assumption of approximately $18 million in existing debt and the remainder in cash. The utility systems serve about 21,000 water and 4,000 wastewater connections in Texas, the release said. Southwest Water Company owns regulated public utilities and also serves cities, utility districts and private companies under contract. More than 2 million people in 35 states are customers of the company, according to the release.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=48994

[Return to top]

Public Health Sector

21. *July 18, Reuters* — **WHO urges bird flu protections for humans. Outbreaks of a deadly bird flu in Asia require tough precautions against the emergence of a new virus strain that could sweep through the human population, the World Health Organisation (WHO) says.** Thailand, the world's fourth largest chicken exporter last year, has seen avian flu hit 15 of 76 provinces over the last two weeks. Since late last year, China, South Korea, Taiwan, Vietnam, Cambodia, and Indonesia also have reported cases. The WHO warned of the possible emergence of a new virus strain that could spark a "global pandemic." Among the precautions WHO urged were protective clothing for workers who might be exposed to the bird flu, which is easily transmitted, and vaccines for those workers. WHO also urged countries with infected flocks to increase surveillance by local and national health officials and to set up procedures for quick sharing of virus samples.
Source: http://www.reuters.co.uk/newsPackageArticle.jhtml?type=world

News&storyID=548931&section=news

22. *July 16, Associated Press* — **Red Cross issues urgent call for blood. The American Red Cross is issuing an urgent call for blood donations, saying parts of the country have less than a day's supply and some hospitals are postponing elective surgeries to conserve.** People with Type O−negative blood, the universal blood type, are particularly needed, but the Red Cross urged anyone who's eligible to donate: people in good health age 17 or older, who weight at least 110 pounds. Summertime blood shortfalls are common, as regular donors go on vacation. The Red Cross calls this year's shortage particularly bad, reporting less than 46,000 units of blood on shelves Thursday, July 15. Anything below 60,000 units is considered a critical shortage; an optimal inventory is 100,000. Two−thirds of Red Cross regions report having less than a day's supply of O−negative blood, said spokesperson Stephanie Millian. **The Red Cross supplies about half the nation's blood.** America's Blood Centers, which supplies the other half, says 20 percent of its reporting centers have a day's supply of blood or less. Source: http://www.baltimoresun.com/features/health/ats−ap_health14jul16,0,306092.story?coll=sns−health−headlines

23. *July 16, International Relations and Security Network (Switzerland)* — **Turkmen doctors fear epidemic.** The outbreak of an infectious pulmonary disease in Turkmenistan that could have been prevented threatens to spiral out of control, doctors warn. **Around a dozen people have died after contracting pneumonic plague, which is similar to its cousin the bubonic plague. While both diseases are spread by rats, the former −− occurring when the untreated bubonic form spreads to the lungs −− is potentially more serious as it is also transmitted by air, and not only by physical contact with an infected creature.** There have been three deaths in the southern Akhal region, near the capital, confirmed by local doctors. A doctor at the main infectious diseases hospital in Ashgabat, who withheld her name, said that one person died on the way to the hospital, “It is a disease that can kill within two hours. The man had a cut on his hand, he and his friends slaughtered an animal, infection got through the wound which led to his death.” A doctor at a district hospital, which had to accommodate the patients initially delivered to the main hospital, said that he witnessed deaths of two more people. The recent deaths followed a May outbreak in the city of Turkmenbashi, leading many to fear that the infection is spreading out of control. Many doctors believe that situation could have been avoided if the authorities had taken appropriate measures back in May of this year. Source: http://www.isn.ethz.ch/infoservice/secwatch/index.cfm?service=cwn&parent=detail&menu=2&sNewsID=9248

24. *July 15, Associated Press* — **CDC: West Nile strikes early, hits the West particularly hard. The early spread of West Nile virus this summer and it's effect on Western states prompted the government Thursday, July 15, to warn Americans to begin taking precautions against the mosquito−borne virus. The virus that returns every summer with mosquito season has already sickened 108 people in 10 states, the Centers for Disease Control and Prevention (CDC) reported.** Three people −− two from Arizona and one from Iowa −− have died. Arizona has had the worst outbreak of any state so far this year, with 66 human cases, followed by California with 20, and Colorado with 12. Thirty−four states in all have reported some form of the virus in either mosquitoes, birds, horses, or people. "We certainly do expect many more cases from around the country to occur in the upcoming weeks ... we're just entering the peak transmission season for the rest of the country," said Lyle

Petersen, director of the CDC's division of vector−borne diseases. Petersen said the agency does not know if the season's early start means there will be more cases this season −− which typically runs through the middle of September −− or if the virus activity will end early.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/nation /9163445.htm

[Return to top]

Government Sector

25. *July 16, Federal Computer Week* — **DHS names directorate CIO. Charles Armstrong has been named the first chief information officer (CIO) at the Department of Homeland Security's (DHS) Border and Transportation Security Directorate.** He will be reporting to Dave Nicholson, resource director at the directorate. Armstrong has been acting CIO at the Bureau of Customs and Border Protection. In his new job, **Armstrong will be in charge of integrating IT across the directorate and overseeing the coordination of major programs,** such as the Automated Commercial Environment (ACE) project, a database that will link every U.S. port of entry and replace a paper−based system, and the U.S. Visitor and Immigrant Status Indicator Technology (US−VISIT) program, DHS' entry/exit system that tracks foreign visitors to the United States. He will be working with Scott Hastings who is the US−VISIT CIO.
Source: http://www.fcw.com/fcw/articles/2004/0712/web−amstr−07−16−04 .asp

[Return to top]

Emergency Services Sector

26. *July 17, Nashua Telegraph (NH)* — **Emergency message startles residents.** This is a test. This is only a test. "That's what I was saying, but it wasn't working," Nashua, NH, Fire Rescue Chief Roger Hatfield explained after a test of a local emergency notification system failed to work as planned. The department, as well as city officials, received calls from residents after Hatfield and Comcast officials conducted a test of the company's emergency notification system, he said. **A text message urging people to contact other media sources for information remained posted on the Nashua cable channels during the hour−long test. However, Hatfield's voice declaring the message a test failed to broadcast.** Hatfield said company officials were attempting to upgrade the system so that both the city's co−emergency management directors, Hatfield and Ed Lecius, as well as Mayor Bernie Streeter could interrupt the cable service when needed to quickly get information to the public. With concerns about emergency preparation for the Democratic National Convention in Boston this month, Hatfield said he and other city officials have been double−checking all of the city's emergency procedures and tools.
Source: http://nsnlb.us.publicus.com/apps/pbcs.dll/article?AID=/2004 0717/NEWS01/207170354/−1/news

27. *July 16, Space Daily* — **Improving incident planning. An enhanced high−tech, collaborative mapping tool is helping law enforcement and emergency management officials better coordinate event and incident planning and real−time response.** The Geographic Tool for Visualization and Collaboration (GTVC) developed by the Georgia Tech

Research Institute proved its usefulness during the G−8 Summit at Sea Island, GA, in June 2004. The Georgia Emergency Management Agency (GEMA) made the tool available to state and federal law enforcement agencies during the event to coordinate their combined resources and responses in real time. GTVC provided many new features for its G−8 use −− including maps with six−inch resolution for G−8 areas of interest. Researchers also added secure encryption for communications. **"Using GTVC, law enforcement teams were able to monitor and track activities in a manner that kept them one step ahead of protestors.** Consequence−management staff also used the system to make sure key resources were available at the right place at the right time. **Furthermore, command staff could immediately get a snapshot of what was going on without relying solely on traditional voice communications,"** said Ralph Reichert, director of GEMA's Terrorism Emergency Preparedness and Response Division.
Source: http://www.spacedaily.com/news/disaster−management−04g.html

[Return to top]

Information Technology and Telecommunications Sector

28. *July 16, eWEEK* — **New Bagle variant heightens alert levels.** A new variant on the Bagle worm has elicited increased alert levels from anti−virus companies. Known as W32/Bagle.af@MM to McAfee, WORM_BAGLE.AF to Trend Micro and W32.Beagle.AB@mm to Symantec, the new version is rated "medium on−watch" by McAfee and "category 3 − moderate" by Symantec. According to Trend Micro, **once executed, the worm drops a copy of itself in the Windows system folder and sets Windows to load it at startup. It uses an internal SMTP mail engine to send copies of itself to addresses that it harvests from a variety of files on the system**. The message may have one of a variety of subject lines and bodies and a spoofed from: address. It also spreads through networks, including peer−to−peer networks, but copying itself to shared folders. **Bagle.AF also attempts to stop running security software on the system and to interfere with copies of the Netsky virus**. Finally, it opens up a back door on port 1080 for attackers to use on the system.
Source: http://www.eweek.com/article2/0,1759,1624336,00.asp

29. *July 15, SearchDomino.com* — **Java applet flaws found in Notes. A trio of newly discovered vulnerabilities in the IBM Lotus Notes R6.x client could put sensitive information on users' PCs at risk**, according Jouko Pynnonen, the independent security consultant who discovered the problems. The vulnerabilities stem from unspecified errors that take place when the Notes client handles Java applets. Pynnonen revealed that the vulnerabilities could be exploited through the sending of harmful Java applets to Notes users via e−mail. "It's when you open an e−mail in Notes that may contain malicious applets," Pynnonen said. Certain applets are handled in such a way that allows a hacker to access certain files on a user's hard disk, and possibly retrieve them surreptitiously via e−mail. Pynnonen said it's unlikely that those looking to spread viruses or worms could successfully exploit the vulnerability because its scope is limited. "It can only read some files, and it can't really do many things; it can't execute any code," Pynnonen said. **IBM posted an acknowledgment of Pynnonen's alleged findings last Friday on its Lotus Support Services Website**. While an official fix is not yet available, Pynnonen said the threat could be eliminated by disabling Java applets.
Source: http://searchdomino.techtarget.com/originalContent/0,289142,sid4_gci992961,00.html

30. *July 15, The Korea Times* — **Seoul plans anti−hacking network in East Asia.** South Korea plans to work together with other Northeast Asian countries including Japan and China to create a joint regional monitoring system against hackers and strengthen cooperation with Australia's Computer Emergency Response Team. The Ministry of Information and Communication (MIC) announced on Thursday, July 15, that it will also form an anti−hacking team with 226 private computer security companies nationwide to promote combined efforts against hacking. **The task force will coordinate between government agencies and private companies, which run many of the nation's information networks, it said. As part of precautionary measures against cross−border cyber terrorism, internet service providers (ISPs) and Internet service operators such as KT and Hanaro Telecom will be required to report any hacking incidents to the MIC.** In addition, the MIC plans to streamline related regulations so that it can make ISPs shut down hackers' access paths and issue hacking warnings. To help small−sized companies, which are particularly vulnerable to network infringement, the MIC will check the systems of 2,400 such firms starting next month. Source: http://times.hankooki.com/lpage/200407/kt2004071516314510440 .htm

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures. **US−CERT Operations Center Synopsis:** Microsoft has released its July Security Updates. Two of these updates are of a critical nature and should be applied to vulnerable systems. For more information, see Microsoft's bulletin here: http://www.microsoft.com/security/bulletins/200407_windows.m spx

Current Port Attacks

Top 10 Target Ports	9898 (dabber), 135 (epmap), 5554 (sasser−ftp), 445 (microsoft−ds), 4899 (radmin), 137 (netbios−ns), 1433 (ms−sql−s), 443 (https), 1434 (ms−sql−m), 8000 (irdmi) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

31. *July 16, Portland Press Herald (ME)* — **Bomb hoax disrupts downtown businesses.** A bomb threat written on the bathroom wall of an Portland (ME) bar earlier this month shut down several downtown businesses and kept hundreds of workers home Thursday, July 15. **Both Portland police and the Federal Bureau of Investigation (FBI) looked into the threat**

against One City Center, a 14−story downtown office building housing the offices of Senator Susan Collins, R−Maine, and found no evidence that the graffiti was more than a hoax, Police Chief Michael Chitwood said Thursday. The threat, written on the wall of a local bar and restaurant on July 6, said there would be a bomb in One City Center on July 15. Police later received an additional report that six men were overheard talking about a bomb in One City Center while they were gathered for the local July 4 fireworks. Police officers and two bomb−sniffing dogs inspected the building Thursday morning as a final precaution, but again found no reason to close it. Nevertheless, the threat was enough to persuade an estimated 80 percent of the business tenants to close for the day, and more than half of the 500 people who work in the building had the day off.
Source: http://business.mainetoday.com/news/040716threat.shtml

32. *July 16, WCPO−TV 9 (OH)* — **Northern Kentucky mall evacuated due to bomb threat.** The Newport on the Levee mall in Newport, KY, was evacuated due to a bomb threat, Friday, July 16. **Police have not released many details about the situation; however, hundreds of people were evacuated and police took canine units inside and allowed some managers to return in order to take the dogs and police through all the departments**. People were told to leave the movie theater, food court and the Newport Aquarium. The Newport Fire Department said it received two separate calls concerning the area. The first was for the mall and the second was for the Newport Aquarium. Newport Police have taken over the investigation in addition to Cincinnati, OH, Police K−9 units. Police plan to search all stores and departments of the mall and aquarium to find out if the threats are credible.
Source: http://www.wcpo.com/news/2004/local/07/16/mall.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.